

RECEIVED
CENTRAL FAX CENTER

ATTORNEY DOCKET NO. SD-6769.1/S96421
SERIAL NO. 09/970,912
PATENT

JUN 05 2006

REMARKS

Claims 1-21 are pending in the application.

Claims 1-21 stand rejected under 35 U.S.C. §102(b) as being anticipated by Michelle L. Hankins, SIGNAL AFCEA'S International Journal, October 1999 "Integrated Circuit Chip Provides Secure, Rapid Data Encryption" ("Hankins").

Applicants respectfully submit that there is nothing enabling in Hankins. Hankins merely reports the existence of an ASIC designed to perform high speed encryption using the DES algorithm. Hankins generally describes pipelining and key-agile pipelined encryption, but does not describe any of the all-important other components and glue as provided by the present invention.

The inventors of the present invention are co-developers of the DES ASIC referenced in the Hankins article, along with Messrs. Pierson and Wilcox and are very familiar with its pipelined architecture and speed potential when used in the Electronic Codebook Mode or the Counter Mode of encryption. The inventors are also keenly aware of its limitations when used in an encryption mode of operation that requires feedback, such as Cipher Block Chaining (CBC). The present application discloses methods that overcome those limitations.

The traditional problem with using pipelined encryptors in a mode of operation requiring feedback, such as CBC Mode, is that the pipeline must be "flushed" or "run dry" on each encryption block in order to obtain an output value to be Exclusively-ORed with the next plaintext block being input to the encryptor. This completely (and usually, more than completely) negates the efficiencies gained by using a pipelined architecture. If there are 18 stages to an encryptor, it can only run at 1/18th of capacity when operating

ATTORNEY DOCKET NO. SD-6769.1/S96421
SERIAL NO. 09/970,912
PATENT

in CBC mode, since it must wait for the first block to progress through all 18 stages before the encrypted result can be fed back and XORed with the second block of plaintext waiting to enter the encryptor pipeline.

The methods put forth in this patent application were developed specifically to be able to exercise the referenced, pipelined, DES ASIC at its full potential in the CBC mode of operation, but are also generally applicable to other pipelined implementations of encryption algorithms and other modes of operation that involve feedback around the encryption engine. They have nothing to do with re-inventing pipelined architectures, only presenting methods for using them more efficiently when using encryption modes of operation requiring feedback. The Hankins article only describes the pipelined nature of the DES ASIC and its ability to be key-agile. It does not disclose how the problem of needing to flush the pipeline between blocks when using a feedback mode of operation, can be overcome. This is disclosed in the present application, but not in Hankins.

Applicants maintain that the methods presented in the present application are not anticipated by Hankins nor would they be obvious to readers of Hankins or others familiar with pipelined encryptors. No one has done this sort of thing; the traditional solution is to wait for the block to make its way through the pipeline, hence losing the efficiency. Also, by the inventors notes and recollections, it took the inventors between 5 and 18 months to figure out just how to manage the initial variables and the values to be fed back to the Exclusive-Or operation. These methods are disclosed in the patent application, but not in Hankins.


ATTORNEY DOCKET NO. SD-6769.1/S96421
SERIAL NO. 09/970,912
PATENT

In view of the foregoing, Applicant respectfully submits that Claims 1-21 are allowable and requests notice to that effect.

Further and favorable consideration is respectfully requested.

Date: 06/05/06

Respectfully submitted,


Madelynn J. Farber
Registration No. 45,410

Sandia National Laboratories
P.O. Box 5800, MS 0161
Albuquerque, NM 87185-0161
(p) 505-844-3858, (f) 505-844-9955